COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 49, No. 2 2000

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

Some Remarks on the Hodge Conjecture for Abelian Varieties of Fermat Type

by

Noboru AOKI

(Received September 18, 2000)

Introduction

Let m be a positive integer greater than two. We denote by X_m^1 the Fermat curve of degree m defined over the complex number field $\mathbb{C}$ by the equation

$$x^m + y^m + z^m = 0\,.$$

Let J_m denote the jacobian variety of X_m^1. An abelian variety over $\mathbb{C}$ is said to be *of Fermat type of degree m* if it is isogenuos to a factor of a power of J_m. In [9], Shioda studied the Hodge conjecture for such abelian varieties. (His definition is slightly more restrictive than that of ours.) He proved, among other things, that if m is a prime number or $m \leq 20$, then the Hodge conjecture is true for all abelian varieties of Fermat type of degree m. We can generalize this as follows.

THEOREM 0.1. *Suppose the prime factorization of m is one of the following forms:*
(i) $m = 2^a 3^b 5^c 7^d$, *where* a, b, c, d *are non-negative integers such that either* $c = 0$ *or* $d = 0$.
(ii) $m = p^e$ *or* $2p^e$, *where* p^e *is a power of an odd prime number* p.
Then the Hodge conjecture is true for all abelian varieties of Fermat type of degree m.

Recall that an abelian variety A defined over $\mathbb{C}$ is said to be a CM abelian variety of type K if K is a CM-field with $[K : \mathbb{Q}] = 2 \dim A$ and if there exists an injective homomorphism $\theta : K \to \mathrm{End}(A) \otimes \mathbb{Q}$. If A is isogenous to a product of a finite number of CM abelian varieties, then we say that A is of CM type ([7]). It is well known that an abelian variety of Fermat type is an example of abelian varieties of CM type.

Let A be an abelian variety of CM type which is isogenous to a product $A_1 \times \cdots \times A_r$ of CM abelian varieties $A_1, \ldots, A_r$ of type $K_1, \ldots, K_r$, respectively. In this paper we say that A is *of cyclotomic type of degree m* if the CM-fields $K_1, \ldots, K_r$ are all abelian fields contained in $\mathbb{Q}(\zeta_m)$, the m-th cyclotomic field. An abelian variety of Fermat type of degree m is known to be of cyclotomic type of degree m. Counting the number of CM-types of the cyclotomic field $\mathbb{Q}(\zeta_m)$, one can easily see that the converse does not hold in

general. However, if $\varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ is small, then the equality "of Fermat type"= "of cyclotomic type" has a chance to hold. Indeed the following theorem holds.

THEOREM 0.2. *If A is a* CM *abelian variety of cyclotomic type of degree m with $\varphi(m) \leq 10$ (hence* $\dim A \leq 5$*), then it is of Fermat type.*

We will see that the assertion of the theorem holds when $\varphi(m) = 12$ except for two CM-types (see Theorem 5.2).

As a consequence of Theorem 0.1, we immediately see that if $\varphi(m) \leq 18$, then the Hodge conjecture is true for any abelian variety of Fermat type of degree m. Combining this with Theorem 0.2, or rather with Theorem 5.1, we can prove the Hodge conjecture for arbitrary powers of a CM abelian variety of type $\mathbb{Q}(\zeta_m)$ provided that $\varphi(m) \leq 12$. But this is not so surprising. Indeed, it is easily verified that such an abelian variety is stably non-degenerate in the sense of Hazama [4], namely the Hodge ring of any power of the abelian variety is generated by divisor classes, and hence the Hodge conjecture is true. However, we also know that a product of some stably non-degenerate CM abelian varieties need not to be stably non-degenerate ([9]). In view of this fact, the following theorem, which is a special case of Theorem 5.2, might be more interesing.

THEOREM 0.3. *Let A be an abelian variety of cyclotomic type which is isogenous to a product $A_1 \times \cdots \times A_n$ of (not necessarily distinct)* CM *abelian varieties $A_1, \ldots, A_n$ satisfying the condition in Theorem* 0.2. *Then the Hodge conjecture is true for A.*

In order to state the next result, we need further notation. Let $\mathfrak{A}_m^1$ be the set of triples (a, b, c) of integers a, b, c such that $0 < a, b, c < m$ and $a + b + c \equiv 0 \pmod{m}$. For each $\alpha = (a, b, c) \in \mathfrak{A}_m^1$ with $\mathrm{GCD}(a, b, c, m) = d$, we denote by C_α the non-singular projective curve over $\mathbb{C}$ whose affine model is defined by the equation

$$y^{m'} = x^{a'}(1 - x)^{b'},$$

where $m' = m/d$, $a' = a/d$ and $b' = b/d$. Then C_α is a quotient of X_m^1 by a subgroup of $\mathrm{Aut}(X_m^1)$. It follows that the jacobian variety J_α of C_α is a factor of J_m, and hence J_α is an abelian variety of Fermat type of degree m. Therefore, if the Hodge conjecture is true for J_m, then so is for J_α. Conversely, since J_m is isogenous to a factor of a product of some of J_α's (see Section 2 for a precise statemant), the Hodge conjecture for *all* J_α implies the Hodge conjecture for J_m. The following theorem asserts that a stronger statement holds.

THEOREM 0.4. *Let $\alpha = (a, b, c)$ be an element of $\mathfrak{A}_m^1$ such that* $\mathrm{GCD}(abc, m) = 1$. *Then the Hodge conjecture for J_α implies the Hodge conjecture for all abelian varieties of Fermat type of degree m.*

As an example, we consider the hyperelliptic curve C_m defined by $y^2 = x^m - 1$ and its jacobian variety $J(C_m)$. Then C_m is a cyclic quotient of X_m^1 and isomorphic to $C_{(1,1,m-2)}$. Thus $J(C_m)$ is isomorphic to $J_{(1,1,m-2)}$. The following corollary to the above theorem might be more impressive.

COROLLARY 0.5. *If m is odd, then the Hodge conjecture for $J(C_m)$ implies the Hodge conjecture for all abelian varieties of Fermat type of degree m.*

1. Hodge cycles on the Fermat varieties

In this section we shall recall some basic results on the Fermat varieties from [8] and [10].

We begin with defining some general notation. Let X be a non-singular projective variety over the complex number field $\mathbb{C}$. For each integer i such that $0 \leq i \leq \dim X$, we denote by

$$\mathcal{B}^i(X) = H^{2i}(X, \mathbb{Q}) \cap H^{i,i}(X)$$

the space of Hodge cycles of codimension i on X. For a subspace V of $\mathcal{B}^i(X)$ (or of $\mathcal{B}^i(X) \otimes \mathbb{C}$), we say that V is *algebraic* if it is generated by fundamental classes of algebraic cycles on X of codimension i. The Hodge conjecture for X asserts that $\mathcal{B}^i(X)$ is algebraic for all i.

The Fermat variety X_m^n over $\mathbb{C}$ of degree m and dimension n is a hypersurface in the $(n+1)$-dimensional projective space $\mathbb{P}^{n+1}$ over $\mathbb{C}$ defined by the equation

$$x_0^m + x_1^m + \cdots + x_{n+1}^m = 0\,.$$

Let μ_m be the group of m-th roots of unity in $\mathbb{C}$ and set $G_m^n = (\mu_m)^{n+2}/\text{diagonal}$. Then $g = [\zeta_0, \ldots, \zeta_{n+1}] \in G_m^n$ acts on X_m^n by letting $g \cdot (x_0 : \ldots : x_{n+1}) = (\zeta_0 x_0 : \ldots : \zeta_{n+1} x_{n+1})$. Hence G_m^n induces an action on the cohomology group $H^n(X_m^n, \mathbb{C})$. Let $(G_m^n)^*$ denote the character group of G_m^n. By the canonical identification $(\mu_m)^* = \mathbb{Z}/m\mathbb{Z}$, we can naturally identify $(G_m^n)^*$ with a subset of $(\mathbb{Z}/m\mathbb{Z})^{n+2}$. For each $\alpha \in (G_m^n)^*$, let

$$V(\alpha) = \{\xi \in H^n(X_m^n, \mathbb{C}) \mid g^*\xi = \alpha(g)\xi \ (\forall g \in G_m^n)\}\,.$$

We define a subset $\mathfrak{A}_m^n$ of $(G_m^n)^*$ as

$$\mathfrak{A}_m^n = \left\{ (a_0, a_1, \ldots, a_{n+1}) \in (\mathbb{Z}/m\mathbb{Z} - \{0\})^{n+2} \;\middle|\; \sum_{i=0}^{n+1} a_i = 0 \right\}.$$

Let $\Gamma_m = (\mathbb{Z}/m\mathbb{Z})^\times$. We have an obvious action of Γ_m on $\mathfrak{A}_m^n$; if $\alpha = (a_0, a_1, \ldots, a_{n+1}) \in \mathfrak{A}_m^n$ and $t \in \Gamma_m$, then

$$t \cdot \alpha = (\langle t a_0 \rangle_m, \ldots, \langle t a_{n+1} \rangle_m)\,,$$

where for any $a \in \mathbb{Z}/m\mathbb{Z}$ and $t \in (\mathbb{Z}/m\mathbb{Z})^\times$, $\langle ta \rangle_m$ denotes the unique integer such that $0 \leq \langle ta \rangle_m < m$ and $\langle ta \rangle_m \equiv ta \pmod{m}$.

We define a subset $\mathfrak{B}_m^n$ of $\mathfrak{A}_m^n$ when n is even. For $\alpha = (a_0, a_1, \ldots, a_{n+1}) \in \mathfrak{A}_m^n$, let

$$|\alpha| = \frac{\langle a_0 \rangle_m + \cdots + \langle a_{n+1} \rangle_m}{m}\,.$$

Clearly $|\alpha|$ is an integer such that $0 < |\alpha| < n+2$. We then define $\mathfrak{B}_m^n$ as

$$\mathfrak{B}_m^n = \left\{ (a_0, \ldots, a_{n+1}) \in \mathfrak{A}_m^n \;\middle|\; |t \cdot \alpha| = \frac{n}{2} + 1 \ (\forall t \in (\mathbb{Z}/m\mathbb{Z})^\times \right\}.$$

THEOREM 1.1. *Let $V(0)$ be the eigenspace corresponding to the trivial character $0 \in (G_m^n)^*$. Then $\dim V(0) = 1$ or 0 according as n is even or odd. The eigenspace*

decomposition of $H^n(X_m^n, \mathbb{C})$ *with respect to the action of* G_m^1 *is given by*

$$H^n(X_m^n, \mathbb{C}) = V(0) \oplus \bigoplus_{\alpha \in \mathfrak{A}_m^n} V(\alpha),$$

where $\dim V(\alpha) = 1$ *for all* $\alpha \in \mathfrak{A}_m^n$. *Moreover, if* $n = 2r$ *is even, then the* $\mathbb{C}$*-span of Hodge cycles of codimension* r *on* X_m^n *is given by*

$$\mathcal{B}^r(X_m^n)_{\mathbb{C}} := \mathcal{B}^r(X_m^n) \otimes_{\mathbb{Q}} \mathbb{C} = V(0) \oplus \bigoplus_{\alpha \in \mathfrak{B}_m^n} V(\alpha).$$

Proof. See [8], [10] or [5]. □

2. Standard elements and the gap group

For $\alpha = (a_0, \dots, a_{n+1}) \in \mathfrak{A}_m^n$ and $\alpha' = (a'_0, \dots, a'_{n'+1}) \in \mathfrak{A}_m^{n'}$, let

$$\alpha * \alpha' = (a_0, \dots, a_{n+1}, a'_0, \dots, a'_{n'+1}) \in \mathfrak{A}_m^{n+n'-2}.$$

Let $\mathfrak{A}_m = \bigsqcup_{n \geq 0} \mathfrak{A}_m^n$ be the disjoint union of $\mathfrak{A}_m^n$ for all $n \geq 0$. Then $\mathfrak{A}_m$ becomes a semigroup with respect to the operation $*$. For two elements $\alpha, \alpha' \in \mathfrak{A}_m$, we write $\alpha \sim \alpha'$ if α is equal to α' up to permutation of components. If $n = 2r$ is even, we define a subset $\mathfrak{D}_m^n$ of $\mathfrak{A}_m^n$ as

$$\mathfrak{D}_m^n = \{\alpha \in \mathfrak{A}_m^n \mid \alpha \sim (a_0, m - a_0, \dots, a_r, m - a_r) \text{ for some } a_0, \dots, a_r\}.$$

It is easy to see that $\mathfrak{D}_m^n \subset \mathfrak{B}_m^n$. Similarly as above, let $\mathfrak{B}_m = \bigsqcup \mathfrak{B}_m^n$ (resp. $\mathfrak{D}_m = \bigsqcup \mathfrak{D}_m^n$) be the disjoint union of $\mathfrak{B}_m^n$ (resp. $\mathfrak{D}_m^n$) for all even $n > 0$.

If m is divisible by a prime number p and $m > p$, then we have explicitly defined elements of $\mathfrak{B}_m$:

$$\sigma_{p,a} = \begin{cases} \left(a, a + \dfrac{m}{p}, a + \dfrac{2m}{p}, \dots, a + \dfrac{(p-1)m}{p}, m - pa\right) & \text{if } p \geq 3, \\ \left(a, a + \dfrac{m}{2}, m - 2a, \dfrac{m}{2}\right) & \text{if } p = 2, \end{cases}$$

where a is an integer such that $0 < a < \frac{m}{p}$. We call $\sigma_{p,a}$ a *standard element*. Let $\mathfrak{S}_m$ be the subset of $\mathfrak{B}_m$ consisting of elemets α for which there exist $\delta, \delta' \in \mathfrak{D}_m$ and standard elements $\sigma_1, \dots, \sigma_r$ such that $\alpha * \delta \sim \sigma_1 * \cdots * \sigma_r * \delta'$. Then we have the following inclusions:

$$\mathfrak{D}_m \subset \mathfrak{S}_m \subset \mathfrak{B}_m \subset \mathfrak{A}_m.$$

Thus, in order to understand the structure of $\mathfrak{B}_m$, it is necessary to know precise imformation of the gap between $\mathfrak{B}_m$ and $\mathfrak{S}_m$. For that purpose, we consider an additive group A_m and its subgroups B_m, S_m and D_m defined in [1] instead of considering $\mathfrak{B}_m$, $\mathfrak{S}_m$ and $\mathfrak{D}_m$ directly. For the convenience of the reader we repeat the definition here.

First, let R_m be the free abelian group generated by the elements of $\mathbb{Z}/m\mathbb{Z} - \{0\}$. An element of R_m will be written as

$$\sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a(a)$$

with $c_a \in \mathbb{Z}$. Next, let

$$A_m = \left\{ \sum_a c_a(a) \in R_m \;\middle|\; \sum c_a = 0 \right\}.$$

Then the map from $\mathfrak{A}_m$ to R_m sending $(a_1, \ldots, a_r)$ to $(a_1) + \cdots + (a_r)$ induces a map

$$u : \mathfrak{A}_m \to A_m .$$

If there is no fear of confusion, we write the image $u((a_1, \ldots, a_r)) \in A_m$ of $(a_1, \ldots, a_r) \in \mathfrak{A}_m$ by the same symbol $(a_1, \ldots, a_r)$. In this notation, we have $u(\alpha * \beta) = \alpha + \beta$ for any $\alpha, \beta \in \mathfrak{A}_m$. Finally, let B_m, S_m and D_m be the subgroup of A_m generated by the $u(\mathfrak{B}_m)$, $u(\mathfrak{S}_m)$ and $u(\mathfrak{D}_m)$ respectively. Then we have inclusions

$$D_m \subset S_m \subset B_m \subset A_m .$$

These abelian groups are all naturally viewed as Γ_m-modules.

For a divisor d of m and $a \in \mathbb{Z}/(m/d)\mathbb{Z}$, we define the "product" $(d)(a)$ to be the element $(a') \in R_m$ such that $a' \equiv da \pmod{m}$. This naturally extends to a map

$$(d) : R_{m/d} \to R_m . \tag{1}$$

To state the strucuture theorem for B_m, we need further notation. Let

$$P = \{4\} \cup \{p \mid p \text{ is an odd prime}\} .$$

For $m > 2$ the equality $\mathfrak{B}_m = \mathfrak{D}_m$, which is equivalent to $B_m = D_m$, holds if and only if $m \in P$ (see [8]). We define a modified Möbius function μ' by

$$\mu'(m) = \begin{cases} (-1)^r & \text{if } m \text{ is a product of } r \text{ distinct elements of } P , \\ 0 & \text{otherwise} . \end{cases}$$

In other words, $\mu'(m) = \mu(m)$ if m is odd, and $\mu'(m) = \mu(m/2)$ if m is even, where μ denotes the usual Möbius function. For example, since $3, 4 \in P$ and $2 \notin P$, we have $\mu'(2) = 0$, $\mu'(3) = \mu'(4) = -1$ and $\mu'(12) = (-1)^2 = 1$.

THEOREM 2.1. *For each divisor $d > 1$ of m such that $\mu'(d) = 1$, there exists an element ξ_d of $B_d - S_d$ with the property that the Γ_m-module B_m is generated by $(m/d)\xi_d$ for all such divisors d of m and S_m. Moreover, we have $2\alpha \in S_m$ for every $\alpha \in B_m$.*

Proof. See [1], Theorem D. □

This theorem gives a necessary and sufficient condition for the equality $\mathfrak{B}_m = \mathfrak{S}_m$ to hold. To state it, we define a subset Q of positive integers as

$$Q = \{p^e \mid p \text{ is a prime and } e \geq 0\} \cup \{2p^e \mid p \text{ is an odd prime and } e \geq 0\} .$$

COROLLARY 2.2. *The equality $\mathfrak{B}_m = \mathfrak{S}_m$ holds if and only if $m \in Q$.*

Proof. Note that $\mathfrak{B}_m = \mathfrak{S}_m$ if and only if $B_m = S_m$. Thus the assertion of the corollary follows from Theorem 2.1 and the fact that there exists a divisor $d > 1$ of m such that $\mu'(d) = 1$ if and only if $m \notin Q$. □

COROLLARY 2.3. *If $\alpha \in \mathfrak{B}_m$, then $\alpha * (t \cdot \alpha) \in \mathfrak{S}_m$ for any $t \in \Gamma_m$.*

Proof. It suffices to show that $\alpha + t \cdot \alpha$ belongs to S_m for all $\alpha \in B_m$. We prove this by induction on m. As is mensioned above, if $m \in P$, then $B_m = D_m$, and so there is nothing to prove. Suppose $m \notin P$, and assume that the assertion is true for any integer m' such that $m' < m$. Let

$$B'_m = S_m + \sum_{\substack{d|m \\ d>1}} (d) B_{m/d} ,$$

where $(d)B_{m/d}$ denotes the image of $B_{m/d}$ under the map (d) defined in (1). Let $\tau : B_m/S_m \to B_m/S_m$ be the map which sends the class of $\alpha \in B_m$ to the class of $\alpha + t \cdot \alpha \in B_m$. We want to show that $\tau = 0$. From the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B'_m/S_m & \longrightarrow & B_m/S_m & \longrightarrow & B_m/B'_m & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tau'} & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau''} & & \\ 0 & \longrightarrow & B'_m/S_m & \longrightarrow & B_m/S_m & \longrightarrow & B_m/B'_m & \longrightarrow & 0 \end{array}$$

with obvious maps τ' and τ'' induced from τ, we obtain an exact sequence

$$0 \to \mathrm{Im}(\tau') \to \mathrm{Im}(\tau) \to \mathrm{Im}(\tau'') . \tag{2}$$

Theorem 2.1 implies that

$$B_m/B'_m \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } \mu'(m) = 1 , \\ 0 & \text{otherwise} . \end{cases}$$

This shows that τ'' is a zero map. To see this, let $\overline{\xi_m}$ be the class of ξ_m in B_m/B'_m. We want to show that $\tau''(\overline{\xi_m}) = 0$. If this were not the case, then B_m would be generated by $\tau(\xi_m)$ and B'_m, and so

$$\tau(\xi_m) \equiv \xi_m \pmod{B'_m} .$$

But this implies that $(t)\xi \equiv 0 \pmod{B'_m}$, which is a contradiction. Hence $\tau''(\overline{\xi_m}) = 0$. Moreover, by the inductive hypothesis, τ' is also a zero map. Therefore $\tau = 0$ by (2), which proves the assertion. □

REMARK 2.4. The quotient group B_m/S_m is called the *gap group*. By Theorem 2.1 one can easily see that

$$B_m/S_m \cong (\mathbb{Z}/2\mathbb{Z})^{2^{r-1}-1}$$

where r is the number of divisors of m belonging to P. This was first proved by Yamamoto in [11], Theorem 4.

3. Abelian varieties of Fermat type

Every element $g \in G^1_m$ induces an automorphism g^* of abelian variety J_m. By Theorem 1.1, we have the eigenspace decomposition of $H^1(J(X^1_m), \mathbb{C})$ with respect to the action of G^1_m:

$$H^1(J(X^1_m), \mathbb{C}) = \bigoplus_{\alpha \in \mathfrak{A}^1_m} U(\alpha) , \tag{3}$$

where $U(\alpha) \cong V(\alpha)$ is one-dimensional for all $\alpha \in \mathfrak{A}_m^1$.

Let $\Omega_m = \Gamma_m \backslash \mathfrak{A}_m^1$ be the orbit space. For $S \in \Omega_m$, let $m_S = m/\mathrm{GCD}(\alpha)$ and ζ_{m_S} a primitive m_S-th root of unity. We define

$$\pi_S = \sum_{g \in G_m^1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{m_S})/\mathbb{Q}}(\alpha(g)) g^* \in \mathrm{End}(J(X_m^1)),$$

where α is an arbitrary chosen element of S. Then the image $A_S = \pi_S(J(X_m^1))$ of J_m under π_S is a CM abelian variety of dimension $\frac{1}{2}\varphi(m_S)$ of type $\mathbb{Q}(\zeta_{m_S})$. Moreover, the eigenspace decomposition of $H^1(A_S, \mathbb{C})$ with respect to the action of G_m^1 is given by

$$H^1(A_S, \mathbb{C}) = \bigoplus_{\alpha \in S} W(\alpha), \tag{4}$$

where $\pi_S^* W(\alpha) = U(\alpha)$. It follows from (3) and (4) that the map

$$\pi = \prod \pi_S : J(X_m^1) \to \prod_{S \in \Omega_m} A_S$$

is an isogeny.

An abelian variety A is said to be *of Fermat type of degree m* if it is isogenous to a factor of a power of J_m, or equivalently if there exist (not necessary distinct) orbits $S_1, \ldots, S_r \in \Omega_m$ and a positive integer k such that

$$A^k \sim A_{S_1} \times \cdots \times A_{S_r}. \tag{5}$$

As is mentioned in the introduction, this definition is slightly more general than that of Shioda [9], where only the case of $k = 1$ is allowded in (5). However, this differnce will not cause any serious problem in this paper since the Hodge conjecture for a power of A implies the Hodge conjecture for A itself.

We now consider Hodge cycles on A. In view of the above remark we consider the case $k = 1$. To state a fundamental theorem due to Shioda [9] on the Hodge cycles on A, we recall some notation. Let $S(A)$ denote the disjoint union of the orbits $S_1, \ldots, S_r$ in (5). If $I = \{\alpha_1, \ldots, \alpha_s\}$ is a subset of $S(A)$, we define a one-dimensional subspace W_I of $H^s(A, \mathbb{C})$ as

$$W_I = W(\alpha_1) \wedge \cdots \wedge W(\alpha_s).$$

Then we can state Shioda's theorem as follows.

THEOREM 3.1. *Let A be an abelian variety of Fermat type of degree m which is isogenuos to the product $A_{S_1} \times \cdots \times A_{S_r}$.*

(i) *The $\mathbb{C}$-span of Hodge cycles on A of codimension d is given by*

$$\mathcal{B}^d(A)_{\mathbb{C}} \cong \bigoplus_I W_I,$$

where the direct sum is taken over the subsets $I = \{\alpha_1, \ldots, \alpha_{2d}\}$ of $S(A)$ such that

$$\alpha_1 * \cdots * \alpha_{2d} \in \mathfrak{B}_m^{6d-2}.$$

(ii) *Let* $I = \{\alpha_1, \dots, \alpha_{2d}\}$ *be a subset of* $S(A)$ *such that* $\alpha_1 * \cdots * \alpha_{2d} \in \mathfrak{B}_m^{6d-2}$. *If the subspace* $V(\alpha_1 * \cdots * \alpha_{2d})$ *of* $\mathcal{B}^{3d-1}(X_m^{6d-2})_{\mathbb{C}}$ *is algebraic, then so is the subspace* W_I *of* $\mathcal{B}^d(A)_{\mathbb{C}}$.

Proof. The first assertion is just a restatement of Theorem 3.1 of [9]. The second assertion follows from Lemma 4.1 and Lemma 4.2 of [loc. cit.]. □

COROLLARY 3.2. *If the Hodge conjecture is true for* X_m^n *for all* n, *then the Hodge conjecture is also true for all abelian varieties of Fermat type of degree* m.

Proof. This is an immediate consequence of Theorem 1.1 and Theorem 3.1. □

For each $\alpha = (a, b, c) \in \mathfrak{A}_m^1$, let C_α and J_α be as in the introduction. Let $\beta = (a_1, \dots, a_s) \in (\mathbb{Z}/m\mathbb{Z} - \{0\})^s$. For each $x \in \mathbb{Z}/m\mathbb{Z}$, we set $(x)\alpha = (xa, xb, xc)$. Moreover, we set

$$\beta\alpha = (a_1)\alpha * \cdots * (a_s)\alpha \in (\mathbb{Z}/m\mathbb{Z})^{3s}.$$

Note that $\beta\alpha \in \mathfrak{A}_m$ if and only if $(a_i)\alpha \in \mathfrak{A}_m^1$ for all $i = 1, \dots, s$. We say that β is *regular* if $a_i \neq a_j$ for all i, j such that $i \neq j$. If β is regular and $\beta\alpha \in \mathfrak{A}_m^{3s-2}$, then we define a one-dimensional subspace $W_\beta(\alpha)$ of $H^s(J_\alpha, \mathbb{C})$ as

$$W_\beta(\alpha) = W_{\{(a_1)\alpha, \dots, (a_s)\alpha\}} = W((a_1)\alpha) \wedge \cdots \wedge W((a_s)\alpha).$$

COROLLARY 3.3. *The* $\mathbb{C}$*-span of the Hodge cycles on* J_α *of codimension* d *is given by*

$$\mathcal{B}^d(J_\alpha)_{\mathbb{C}} = \bigoplus_\beta W_\beta(\alpha),$$

where the direct sum is taken over the regular elements $\beta \in (\mathbb{Z}/m\mathbb{Z} - \{0\})^{2d}$ *such that* $\beta\alpha \in \mathfrak{B}_m^{6d-2}$.

Proof. This is a special case of Theorem 3.1. To be more precise, let $\{d_1 \dots, d_r\}$ be the set of divisors d of m such that $(d)\alpha \in \mathfrak{A}_m^1$, namely $da \not\equiv 0$, $db \not\equiv 0$, $dc \not\equiv 0 \pmod m$. Let S_i be the orbit of $(d_i)\alpha$. Then we have

$$J_\alpha \sim \prod_{i=1}^r A_{S_i},$$

and so $S(J_\alpha) = \{(a)\alpha \mid a \in \mathbb{Z}/m\mathbb{Z}, (a)\alpha \in \mathfrak{A}_m^1\}$. It follows that any subset I of $S(J_\alpha)$ of order $2d$ is of the form

$$I = \{(a_1)\alpha, \dots, (a_{2d})\alpha\},$$

where $(a_1, \dots, a_{2d}) \in (\mathbb{Z}/m\mathbb{Z} - \{0\})^{2d}$ is a regular element such that $(a_i)\alpha \in \mathfrak{A}_m^1$ for all $i = 1, \dots, 2d$. Thus I corresponds uniquely to a regular element $\beta \in (\mathbb{Z}/m\mathbb{Z} - \{0\})^{2d}$ such that $\beta\alpha \in \mathfrak{A}_m^{6d-2}$. Therefore the asserion of the corollary follows from Theorem 3.1. □

4. Proof of Theorem 0.1

For the proof of Theorem 0.1 we need a lemma below.

LEMMA 4.1. *Let $\alpha, \beta \in \mathfrak{B}_m$. Then the following statements hold.*

(i) *If both $V(\alpha)$ and $V(\beta)$ are algebraic, then so is $V(\alpha * \beta)$.*

(ii) *If $V(\alpha * \delta)$ is algebraic for some $\delta \in \mathfrak{D}_m$, then so is $V(\alpha)$.*

(iii) *If $\alpha \in \mathfrak{S}_m$, then $V(\alpha)$ is algebraic.*

Proof. The first and second statements are proved in [8], Corollary to Theorem II and Lemma 3, respectively. The third statement is proved using the results of [5], [8] and [2]. For the convenience of the reader, we present here an outline of the proof. If $\alpha \in \mathfrak{D}_m^n$, then it is known that $V(\alpha)$ is generated by classes of some linear spaces on X_m^n ([5], [8]). Moreover, it is proved that $V(\sigma_{p,a})$ is algebraic for every standard element $\sigma_{p,a}$ ([2]). As for general $\alpha \in \mathfrak{S}_m$, the algebraicity of $V(\alpha)$ follows from (i), (ii) and the results above on the standard elements. □

Proof of Theorem 0.1. In view of Corollary 3.2, it suffices to show that the Hodge conjecture for X_m^n is true for all n when m satisfies one of the condition of the theorem. First, if $m \in Q$, then $\mathfrak{B}_m = \mathfrak{S}_m$ by Corollary 2.2. Therefore Lemma 4.1 implies that $V(\alpha)$ is algebraic for all $\alpha \in \mathfrak{B}_m$, and hence the Hodge conjectura for X_m^n is true for all n. This proves the first assertion of the theorem.

Next, we consider the case where m satisfies the first condition of the theorem. In this case, by Lemma 4.1 and Theorem 2.1, it suffices to verify the algebraicity of $V(\xi)$ for $\xi = \xi_m$ with $m = 12, 15, 20, 21, 28$, where

$$\xi_m = \begin{cases} (1, 6, 8, 9) & (m = 12), \\ (1, 6, 10, 13) & (m = 15), \\ (1, 4, 17, 18) & (m = 20), \\ (1, 4, 16, 9, 15, 18) & (m = 21), \\ (1, 9, 25, 12, 20, 24) & (m = 28) \end{cases}$$

are generators of the gap group (see Theorem 2.1). Note that ξ_m belongs to $\mathfrak{B}_m^2 \cup (\mathfrak{B}_m^4 \cap (\mathfrak{A}_m^1 * \mathfrak{A}_m^1))$. Since $V(\alpha)$ is albebraic for every $\alpha \in \mathfrak{B}_m^2 \cup (\mathfrak{B}_m^4 \cap (\mathfrak{A}_m^1 * \mathfrak{A}_m^1))$ (see the proof of Theorem 4.3 of [9]), $V(\xi_m)$ are all algebraic. This completes the proof. □

5. Abelian varieties of cyclotomic type

In this section K will always denote an imaginary abelian field such that $K \subset \mathbb{Q}(\zeta_m)$ and A a CM abelian variety of type K. Let $\theta : K \to \mathrm{End}(A) \otimes \mathbb{Q}$ be the embedding giving the complex multiplication.

LEMMA 5.1. *Notation being as above, let $[\mathbb{Q}(\zeta_m) : K] = n$. Then A^n is a* CM *abelian variety of type $\mathbb{Q}(\zeta_m)$.*

Proof. Let $\rho : \mathbb{Q}(\zeta_m) \to M_n(K)$ be the regular representation of $\mathbb{Q}(\zeta_m)$ over K. Composing ρ with the inclusion map

$$M_n(K) \hookrightarrow M_n(\mathrm{End}(A) \otimes \mathbb{Q}) \subset \mathrm{End}(A^n) \otimes \mathbb{Q}$$

induced from θ, we obtain an injective homomorophism of $\mathbb{Q}$-algebra

$$\theta' : \mathbb{Q}(\zeta_m) \to \mathrm{End}(A^n) \otimes \mathbb{Q}\,.$$

Since $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = n[K : \mathbb{Q}] = 2 \dim A^n$, this shows that A^n is a CM abelian variety of type $\mathbb{Q}(\zeta_m)$. □

In the following, we identify the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ with $\Gamma_m = (\mathbb{Z}/m\mathbb{Z})^\times$ in the usual manner. Under this identification, a CM type Φ of $\mathbb{Q}(\zeta_m)$ is by definition a subset of Γ_m such that $\Phi \cup (-1)\Phi = \Gamma_m$ and $\Phi \cap (-1)\Phi = \emptyset$.

For two CM-types Φ and Φ' of K, we say that Φ is equivalent to Φ' if $\Phi = (t) \cdot \Phi'$ for some $t \in \Gamma_m$.

THEOREM 5.2. *Let K be an imaginary abelian field contained in $\mathbb{Q}(\zeta_m)$ with $\varphi(m) \leq 12$. Let A be a* CM *abelian variety of type K and (K, Φ) the* CM*-type of (A, θ).*

(i) *If $K \neq \mathbb{Q}(\zeta_{13}), \mathbb{Q}(\zeta_{28})$, then A is an abelian variety of Fermat type.*

(ii) *If $K = \mathbb{Q}(\zeta_{13}), \mathbb{Q}(\zeta_{28})$ and if the* CM*-type Φ is not equivalent to a* CM*-type Φ_0, where*

$$\Phi_0 = \begin{cases} \{1, 3, 4, 5, 7, 11\} & (K = \mathbb{Q}(\zeta_{13}))\,, \\ \{1, 5, 9, 11, 15, 25\} & (K = \mathbb{Q}(\zeta_{28}))\,, \end{cases}$$

then A is an abelian variety of Fermat type.

Note that for $g \leq 6$ the integers m such that $\varphi(m)/2 = g$ and $\mathrm{ord}_2(m) \neq 1$ are given as follows:

g	m			
1	3	4		
2	5	8	12	
3	7	9		
4	15	16	20	24
5	11			
6	13	21	28	36

Proof of Theorem 5.2. In view of the above lemma, it suffices to consider only the case $K = \mathbb{Q}(\zeta_m)$. Let A_S be an abelian variety of Fermat type defined in Section 3 and $\theta_S : \mathbb{Q}(\zeta_m) \to \mathrm{End}(A_S) \otimes \mathbb{Q}$ the injection giving the complex multiplication. We can choose an element $\alpha = (a, b, c) \in S$ so that $\theta(\alpha(g)) = g^*$ for all $g \in G_m^1$. The CM-type of (A_S, θ_S) is then given by

$$\Phi_\alpha = \{t \in (Z/m\mathbb{Z})^\times \mid \langle ta \rangle_m + \langle tb \rangle_m + \langle tc \rangle_m = m\}\,, \tag{6}$$

where $\langle ta \rangle_m$ denotes the integers defined in Section 1. By a general theorem of CM abelian varieties, A is isogenous to A_S if and only if Φ is equivalent to Φ_α (see [7]). Therefore, in order to prove the theorem, we have only to find an element $\alpha \in \mathfrak{A}_m^1$ such that $\Phi_\alpha = \Phi$. The result is given in the table in the final section. Note that the table shows that if Φ is equivalent to Φ_0, then A is not of Fermat type. □

THEOREM 5.3. *Let A be an abelian variety of cyclotomic type which is isogenous to a product $A_1 \times \cdots \times A_n$ of (not necessarily distinct)* CM *abelian varieties $A_1, \ldots, A_n$ of type $K_1, \ldots, K_r$, respectively, for which the following conditions holds.*

(i) *For each i, the* CM*-field K_i is contained in a cyclotomic field $\mathbb{Q}(\zeta_{m_i})$ with $\varphi(m_i) \leq 12$.*

(ii) *If $n > 1$, then none of the* CM*-types of A_i's is equivalent to Φ_0 in Theorem* 5.2.

Then the Hodge conjecture is true for A.

Proof. This is an immediate consequence of Theorem 0.1 and Theorem 5.2. □

REMARK 5.4. New ideas will be needed when we try to prove the Hodge conjecture for a CM abelian variety A of cyclotomic type with $\dim A = 8$. This is because there exist degenerate CM abelian varieties which are of cyclotomic type and not of Fermat type. For example if $K = \mathbb{Q}(\zeta_{32})$ and

$$\Phi = \{1, 7, 13, 15, 21, 23, 27, 29\},$$

then an abelian variety of type K with CM-type Φ is degenerate and not of Fermat type. This example is due to Lenstra (see [6]).

6. Proof of Theorem 0.4

If the Hodge conjecture for X_m^n is true for all n, then the Hodge conjecture for any abelian variety of Fermat type of degree m is also true ([9]). Thus Theorem 0.4 directly follows from this fact and the following theorem.

THEOREM 6.1. *Let $\alpha = (a, b, c)$ be an element of $\mathfrak{A}_m^1$ such that* $\mathrm{GCD}(abc, m) = 1$. *Then the Hodge conjecture for $J(C_\alpha)$ implies the Hodge conjecture for all Fermat varieties of degree m.*

Before proving this theorem, we prove a lemma which will play a key role in the proof of the theorem. To state it we define some notation. Let l, m be positive integers such that $l < m$. We identify $\mathbb{Z}/m\mathbb{Z}$ with the subset $\{0, 1, \ldots, m-1\}$ of $\mathbb{Z}$ with the usual linear order. Thus, considering the lexicographic order, we can view the direct product $(\mathbb{Z}/m\mathbb{Z})^l$ as a linearly ordered set. We define two subsets S_l and T_l of $(\mathbb{Z}/m\mathbb{Z})^l$. First, let S_l be the permutation group of l elements $\{1, 2, \ldots, l\}$. Pulling back the order of $(\mathbb{Z}/m\mathbb{Z})^l$ by the injection $S_l \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^l$ sending σ to $(\sigma(1), \ldots, \sigma(l))$, we define a linear order on S_l. Let $\sigma_1 < \sigma_1 < \cdots < \sigma_{l!}$ be the ordering of the elements of S_l. Next, we define T_l by

$$T_l = \{\tau = (t_1, \ldots, t_l) \in (\mathbb{Z}/m\mathbb{Z})^l \mid 0 \leq t_i \leq i - 1 \ (i = 1, \ldots, l)\}.$$

Clearly $|T_l| = l!$. Let $\tau_1 < \tau_1 < \cdots < \tau_{l!}$ be the ordering of the elements of T_l.

Now, fix an element $\alpha = (a_1, \dots, a_l) \in (\mathbb{Z}/m\mathbb{Z} - \{0\})^l$. We let S_l act on α by

$$\sigma(\alpha) = (a_{\sigma(1)}, \dots, a_{\sigma(l)}) .$$

Obviously $\sigma(\alpha)$'s are all distinct if and only if α is regular in the sense of Section 3, i.e., $a_i \neq a_j$ for $i \neq j$. Let

$$\langle\ ,\ \rangle : (\mathbb{Z}/m\mathbb{Z})^l \times (\mathbb{Z}/m\mathbb{Z})^l \to \mathbb{Z}/m\mathbb{Z}$$

be the usual inner product on $(\mathbb{Z}/m\mathbb{Z})^l$.

LEMMA 6.2. *Let ζ be a primitive m-th root of unity. For $\alpha \in \mathbb{Z}^l$, we define a square matrix $Y_l(\alpha) = Y_l(\alpha, \zeta)$ of size $l!$ by*

$$Y_l(\alpha) = (\zeta^{\langle \sigma(\alpha), \tau \rangle})_{\substack{\sigma \in S_l \\ \tau \in T_l}} = (\zeta^{\langle \sigma_p(\alpha), \tau_q \rangle})_{1 \leq p,q \leq l!} .$$

Then the determinant of $Y_l(\alpha)$ is calculated as

$$\det(Y_l(\alpha)) = \left\{ \prod_{1 \leq i < j \leq l} (\zeta^{a_i} - \zeta^{a_j}) \right\}^{l!} ,$$

where the right hand side is regarded to be 1 when $l = 1$. In particular, $Y_l(\alpha)$ is regular if and only if α is regular.

Proof. We prove this by induction on l. If $l = 1$ then the lemma is clear since $Y_1(a) = 1$ for any $a \in \mathbb{Z}/m\mathbb{Z}$. Let $l > 1$ and assume that

$$\det(Y_{l-1}(\beta)) = \left\{ \prod_{1 \leq i < j \leq l-1} (\zeta^{b_i} - \zeta^{b_j}) \right\}^{(l-1)!}$$

for any $\beta = (b_1, \dots, b_{l-1}) \in (\mathbb{Z}/m\mathbb{Z} - \{0\})^{l-1}$.

For each $i = 1, \dots, l$, let

$$\begin{cases} S_l(i) = \{\sigma \in S_l \mid \sigma(l) = i\} , \\ T_l(i) = \{(t_1, \dots, t_l) \in T_l \mid t_l = i\} . \end{cases}$$

Then we have decompositions of S_l and T_l:

$$S_l = \bigsqcup_{1 \leq i \leq l} S_l(i) , \quad T_l = \bigsqcup_{1 \leq i \leq l} T_l(i) .$$

According to these decompositions, we write $Y_l(\alpha)$ as

$$Y_l(\alpha) = \begin{pmatrix} Y_l(\alpha)_{11} & \cdots & Y_l(\alpha)_{1l} \\ \vdots & & \vdots \\ Y_l(\alpha)_{l1} & \cdots & Y_l(\alpha)_{ll} \end{pmatrix} ,$$

where the (i, j)-block $Y_l(\alpha)_{ij}$ is a square matrix of size $(l-1)!$ defined by

$$Y_l(\alpha)_{ij} = (\zeta^{\langle \sigma(\alpha), \tau \rangle})_{\substack{\sigma \in S_l(i) \\ \tau \in T_l(j)}} .$$

If $\sigma \in S_l(i)$ and $\tau = (t_1, \ldots, t_{l-1}, j) \in T_l(j)$, then

$$\begin{aligned}\langle \sigma(\alpha), \tau \rangle &= a_{\sigma(1)} t_1 + \cdots + a_{\sigma(l-1)} t_{l-1} + a_i j \\ &= \langle \sigma'(\alpha_{(i)}), \tau' \rangle + a_i j\,,\end{aligned}$$

where $\alpha_{(i)} = (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_l) \in (\mathbb{Z}/m\mathbb{Z} - \{0\})^{l-1}$, $\sigma' \in S_{l-1}$ is the restriction of σ to the subset $\{1, \ldots, l-1\}$ of $\{1, \ldots, l\}$ and $\tau' = (t_1, \ldots, t_{l-1}) \in T_{l-1}$. Hence

$$Y_l(\alpha)_{ij} = (\zeta^{a_i})^j Y_{l-1}(\alpha_{(i)})\,.$$

Therefore

$$Y_l(\alpha) = \begin{pmatrix} Y_{l-1}(\alpha_{(1)}) & \cdots & O \\ \vdots & \ddots & \vdots \\ O & \cdots & Y_{l-1}(\alpha_{(l)}) \end{pmatrix} \left(\begin{pmatrix} 1 & \zeta^{a_1} & \cdots & (\zeta^{a_1})^{l-1} \\ \vdots & \vdots & & \vdots \\ 1 & \zeta^{a_l} & \cdots & (\zeta^{a_l})^{l-1} \end{pmatrix} \otimes E_{(l-1)!} \right), \tag{7}$$

where $E_{(l-1)!}$ denotes the unit matrix of size $(l-1)!$. By the inductive hypothesis we have

$$\det(Y_l(\alpha_{(i)})) = \prod_{\substack{1 \le \mu < \nu \le l-1 \\ \mu, \nu \ne i}} \{(\zeta^{a_\mu} - \zeta^{a_\nu})\}^{(l-1)!} \tag{8}$$

for all $i = 1, \ldots, l$. It follows from (7) and (8) that

$$\begin{aligned}\det(Y_l(\alpha)) &= \prod_{i=1}^{l} \left\{ \prod_{\substack{1 \le \mu < \nu \le l-1 \\ \mu, \nu \ne i}} (\zeta^{a_\mu} - \zeta^{a_\nu}) \right\}^{(l-1)!} \left\{ \det \begin{pmatrix} 1 & \zeta^{a_1} & \cdots & (\zeta^{a_1})^{l-1} \\ \vdots & \vdots & & \vdots \\ 1 & \zeta^{a_l} & \cdots & (\zeta^{a_l})^{l-1} \end{pmatrix} \right\}^{(l-1)!} \\ &= \prod_{i=1}^{l} \left\{ \prod_{\substack{1 \le \mu < \nu \le l-1 \\ \mu, \nu \ne i}} (\zeta^{a_\mu} - \zeta^{a_\nu}) \right\}^{(l-1)!} \left\{ \prod_{1 \le \mu < \nu \le l-1} (\zeta^{a_\mu} - \zeta^{a_\nu}) \right\}^{(l-1)!} \\ &= \left\{ \prod_{1 \le \mu < \nu \le l} (\zeta^{a_\mu} - \zeta^{a_\nu}) \right\}^{(l-1)(l-1)!} \left\{ \prod_{1 \le \mu < \nu \le l} (\zeta^{a_\mu} - \zeta^{a_\nu}) \right\}^{(l-1)!} \\ &= \left\{ \prod_{1 \le \mu < \nu \le l} (\zeta^{a_\mu} - \zeta^{a_\nu}) \right\}^{l!}\,.\end{aligned}$$

Clearly, $\det(Y_l(\alpha)) \ne 0$ if and only if $a_\mu \ne a_\nu$ for all μ, ν with $\mu \ne \nu$. This completes the proof of Lemma 6.2. □

PROPOSITION 6.3. *Let $\alpha = (a, b, c)$ be an element of $\mathfrak{A}_m^1$ such that* $\mathrm{GCD}(abc, m) = 1$. *Let d be a positive integer such that $2d < m$ and $\beta = (a_1, \ldots, a_{2d})$ a regular element of $(\mathbb{Z}/m\mathbb{Z} - \{0\})^{2d}$ such that $\alpha\beta \in \mathfrak{B}_m^{6d-2}$. If the subspace $W_\beta(\alpha)$ of $\mathcal{B}^d(J_\alpha)_{\mathbb{C}}$ is algebraic, then so is the subspace $V(\beta\alpha)$ of $\mathcal{B}^{3d-1}(X_m^{6d-2})_{\mathbb{C}}$.*

Proof. Consider the one-dimensional subspace

$$V_\beta(\alpha) := V((a_1)\alpha) \otimes \cdots \otimes V((a_{2d})\alpha)$$

of $\mathcal{B}^d(C_\alpha^{2d})_{\mathbb{C}}$. Then Shioda's inductive structure provides an isomorophism $V_\beta(\alpha) \cong V(\beta\alpha)$ which preserves algebraicity ([8]). Hence it suffices to show that if $W_\beta(\alpha)$ is algebraic, then so is $V_\beta(\alpha)$. (This is a counterpart of Theorem 3.1, (ii).)

Now, the permutation group S_{2d} naturally acts on C_α^{2d}, and an element $\sigma \in S_{2d}$ induces an endomorphism σ^* on $H^d(C_\alpha^{2d}, \mathbb{C})$. Let ω be a non-zero element of $V_\beta(\alpha)$ and put

$$\eta = \sum_{\sigma \in S_{2d}} \sigma^*(\omega) \in H^{2d}(C_\alpha^{2d}, \mathbb{C})^{S_{2d}} .$$

Let $\varphi_{2d} : C_\alpha^{2d} \to J_\alpha$ be the natural map induced from the canonical map $\varphi : C_\alpha \to J_\alpha$. Then $\eta \in \varphi_{2d}^*(W_\beta(\alpha))$. Since $W_\beta(\alpha)$ is algebraic, this shows that η is algebraic.

Let g be an element of G_m^1 such that $\alpha(g)$ is a primitive m-th root of unity. The existance of such an automorphism g is assured by the assumption that $\mathrm{GCD}(abc, m) = 1$. For $\tau = (t_1, \dots, t_{2d}) \in T_{2d}$, let $g_\tau = (g^{t_1}, \dots, g^{t_{2d}}) \in \mathrm{Aut}(C_\alpha^{2d})$. Then $g_\tau^*(\sigma^*(\omega)) = \alpha(g)^{\langle \sigma(\beta), \tau \rangle} \sigma^*(\omega)$ for any $\sigma \in S_{2d}$, and so

$$g_\tau^*(\eta) = \sum_{\sigma \in S_{2d}} \alpha(g)^{\langle \sigma(\beta), \tau \rangle} \sigma^*(\omega) .$$

Therefore, putting $N = (2d)!$, we have

$$\begin{pmatrix} g_{\tau_1}^*(\eta) \\ \vdots \\ g_{\tau_N}^*(\eta) \end{pmatrix} = Y_{2d}(\beta) \begin{pmatrix} \sigma_1^*(\omega) \\ \vdots \\ \sigma_N^*(\omega) \end{pmatrix} ,$$

where $Y_{2d}(\beta) = Y_{2d}(\beta, \alpha(g))$ is the matrix defined in Lemma 6.2 for $\zeta = \alpha(g)$. Since $\alpha(g)$ is a primitive m-th root of unity and β is regular, Lemma 6.2 shows that $Y_{2d}(\beta)$ is regular. Hence $\sigma^*(\omega)$ can be expressed as a linear combination of $g_\tau^*(\eta)$ ($\tau \in T_{2d}$) for any $\sigma \in S_{2d}$. This, in particular, shows that ω (and hence $V_\beta(\alpha)$) is algebraic. □

Proof of Theorem 6.1. Let $\alpha = (a, b, c) \in \mathfrak{A}_m^1$ and suppose that $\mathrm{GCD}(abc, m) = 1$. Without loss of generality we may assume that $a = 1$. We want to prove that $V(\xi)$ is algebraic for any generator ξ of $\mathfrak{B}_m$. To do this we may assume that ξ is regular. Since $\xi\alpha \in \mathfrak{B}_m$, $W_\xi(\alpha)$ is algebraic by the assumption of the theorem. Then the Proposition 6.3 shows that $V(\xi\alpha)$ is also algebraic. Here we note that

$$\xi\alpha \sim \xi * (b)\xi * (c)\xi .$$

If we put $\delta = (b)\xi * (c)\xi * (-b)\xi * (-c)\xi \in \mathfrak{D}_m$, then this implies that

$$\xi * \delta \sim (\xi\alpha) * (-b)\xi * (-c)\xi .$$

Since $(-b)\xi * (-c)\xi = (-b)(\xi * (b^{-1}c)\xi)$ belongs to $\mathfrak{S}_m$ by Corollary 2.3, this shows that $V(\xi * \delta)$ is algebraic by Lemma 4.1. Therefore $V(\xi)$ is algebraic by the same lemma. □

7. List of CM-types of small cyclotomic fields

In the table below, for each integer $m > 2$ with $\varphi(m) \leq 12$, we listed all inequivalent CM-types Φ for $\mathbb{Q}(\zeta_m)$ and all inequivalent elemets $\alpha = (a, b, c) \in \mathfrak{A}_m^1$ such that $\mathrm{GCD}(a, b, c, m) = 1$ and $\Phi = \Phi_\alpha$, where Φ_α denotes a CM-type defined by (6). (Here, similarly as in the case of Φ, we say that an element $\alpha \in \mathfrak{A}_m^1$ is equivalent to another $\alpha' \in \mathfrak{A}_m^1$ if $t \cdot \alpha \sim \alpha'$ for some $t \in \Gamma_m$.) In the table, a CM-type Φ of $\mathbb{Q}(\zeta_m)$ is asterisked if m is odd and there is no element $\alpha \in \mathfrak{A}_m^1$ such that $\Phi = \Phi_\alpha$ but $\Phi = \Phi_{\alpha'} \pmod m$ for some $\alpha' \in \mathfrak{A}_{2m}^1$. (Note that $\Gamma_m \cong \Gamma_{2m}$ when m is odd.) For example, for $m = 11$ and $\Phi = \{1, 2, 3, 5, 9\}$ there is no element $\alpha \in \mathfrak{A}_{11}^1$ such that $\Phi = \Phi_\alpha$ but $\Phi = \Phi_{(1,2,19)} \pmod{11}$ for $(1, 2, 19) \in \mathfrak{A}_{22}^1$.

We calculated the "level" of Φ, denoted by $m(\Phi)$ in the table, which is defined to be the largest divisor m' of m for which Φ comes from a CM-type Φ' of $\mathbb{Q}(\zeta_{m'})$, i.e.,

$$\Phi = \mathrm{cor}_{\Gamma_m/\Gamma_{m'}}(\Phi'),$$

where $\mathrm{cor} : \mathbb{Z}[\Gamma_{m'}] \to \mathbb{Z}[\Gamma_m]$ denotes the corestriction map. Consider the case where $m(\Phi) = m' < m$ and $\Phi = \mathrm{cor}_{\Gamma_m/\Gamma_{m'}}(\Phi')$ for a CM-type Φ' of $\mathbb{Q}(\zeta_{m'})$. If $\Phi' = \Phi_{\alpha'}$ for some $\alpha' \in \mathfrak{A}_{m'}^1$, then $\Phi = \Phi_\alpha$ with $\alpha = (m/m')\alpha' \in \mathfrak{A}_m^1$. For example, in the case of $m = 9$ and $\Phi = \{1, 4, 7\}$ the blank in the table means that there is no element $\alpha \in \mathfrak{A}_9^1$ with $\mathrm{GCD}(\alpha) = 1$ such that $\Phi = \Phi_\alpha$. But we have $\Phi = \Phi_{(3,3,3)}$ for $(3, 3, 3) \in \mathfrak{A}_9^1$. This corresponds to the fact that $\Phi = \mathrm{cor}_{\Gamma_9/\Gamma_3}(\Phi')$ with $\Phi' = \Phi_{(1,1,1)} = \{1\}$. Thus, in order to prove Theroem 5.2, we have only to consider CM-types Φ such that $m(\Phi) = m$.

We also calculated the automorphism group $W(\Phi)$ of Φ, which is defiened by

$$W(\Phi) = \{t \in \Gamma_m \mid t \cdot \Phi = \Phi\}.$$

It is well known that A is simple if and only if $W(\Phi)$ is trivial; more generally A is isogenous to the product of $\#W(\Phi)$ copies of a simple CM abelian variety of type $\mathbb{Q}(\zeta_m)^{W(\Phi)}$.

m	Φ	$m(\Phi)$	$W(\Phi)$	α
3	$\{1\}$	3	$\{1\}$	$(1, 1, 1)$
4	$\{1\}$	4	$\{1\}$	$(1, 1, 2)$
5	$\{1, 2\}$	5	$\{1\}$	$(1, 1, 3)$
7	$\{1, 2, 3\}$	7	$\{1\}$	$(1, 1, 5)$
	$\{1, 2, 4\}$	7	Φ	$(1, 2, 4)$
8	$\{1, 3\}$	8	Φ	$(1, 1, 6)$ $(1, 3, 4)$
	$\{1, 5\}$	4	Φ	$(1, 2, 5)$
9	$\{1, 2, 4\}$	9	$\{1\}$	$(1, 1, 7)$ $(1, 3, 5)$
	$\{1, 4, 7\}$	3	Φ	

m	Φ	$m(\Phi)$	$W(\Phi)$	α
11	{1, 2, 3, 4, 5}	11	{1}	(1, 1, 9)
	{1, 2, 3, 4, 6}	11	{1}	(1, 4, 6)
	{1, 2, 3, 5, 7}*	11	{1}	(1, 2, 19)
	{1, 3, 4, 5, 9}*	11	Φ	(1, 3, 18)
12	{1, 5}	4	Φ	(1, 1, 10) (1, 3, 8) (1, 5, 6)
	{1, 7}	3	Φ	(1, 2, 9) (1, 4, 7)
13	{1, 2, 3, 4, 5, 6}	13	{1}	(1, 1, 11)
	{1, 2, 3, 4, 5, 7}*	13	{1}	(1, 2, 23)
	{1, 2, 3, 4, 6, 8}	13	{1}	(1, 5, 7)
	{1, 2, 3, 5, 6, 9}	13	{1, 3, 9}	(1, 3, 9)
	{1, 2, 3, 5, 7, 9}	13	{1}	(1, 4, 21) (1, 9, 16)
	{1, 2, 6, 8, 9, 10}	13	{1}	
15	{1, 2, 4, 7}	15	{1}	(1, 1, 13) (1, 5, 9)
	{1, 2, 4, 8}	15	Φ	(1, 2, 12) (1, 4, 10)
	{1, 2, 7, 11}	5	{1, 11}	(1, 3, 11)
	{1, 4, 7, 13}	3	Φ	
16	{1, 3, 5, 7}	16	{1, 7}	(1, 1, 14) (1, 7, 8)
	{1, 3, 5, 9}	16	{1}	(1, 2, 13) (1, 4, 11)
	{1, 3, 9, 11}	8	Φ	(1, 6, 9)
	{1, 5, 9, 13}	4	Φ	
20	{1, 3, 7, 9}	20	Φ	(1, 1, 8) (1, 3, 16) (1, 9, 10)
	{1, 3, 7, 11}	20	{1}	(1, 4, 15) (2, 3, 15)
	{1, 3, 11, 13}	5	{1, 11}	(1, 2, 17) (1, 8, 11)
	{1, 9, 13, 17}	4	Φ	
21	{1, 2, 4, 5, 8, 10}	21	{1}	(1, 1, 19) (1, 3, 17) (1, 9, 11)
	{1, 2, 4, 5, 8, 11}	21	{1}	(1, 6, 14)
	{1, 2, 4, 5, 10, 13}	21	{1, 13}	(1, 7, 13)
	{1, 2, 4, 8, 11, 16}	7	Φ	(1, 4, 16) (1, 8, 12)
	{1, 2, 4, 10, 13, 16}*	21	{1}	(2, 7, 33) (7, 11, 24) (7, 13, 22)
	{1, 2, 5, 8, 10, 17}*	21	{1}	(1, 4, 27)
	{1, 2, 8, 10, 16, 17}	7	{1, 8}	
	{1, 4, 10, 13, 16, 19}	3	Φ	

m	Φ	$m(\Phi)$	$W(\Phi)$	α			
24	{1, 5, 7, 11}	24	Φ	(1, 1, 22)	(1, 5, 18)	(1, 7, 16)	(1, 11, 12)
	{1, 5, 7, 13}	24	{1}	(1, 2, 21)	(1, 8, 15)	(2, 7, 15)	(4, 5, 15)
	{1, 5, 13, 17}	4	Φ	(1, 6, 17)	(1, 10, 13)		
	{1, 7, 13, 19}	3	Φ	(1, 4, 19)			
	{1, 11, 17, 19}	8	Φ				
28	{1, 3, 5, 9, 11, 13}	28	{1, 13}	(1, 1, 26)	(1, 13, 14)		
	{1, 3, 5, 9, 11, 15}	28	{1}	(1, 4, 23)	(1, 8, 19)		
	{1, 3, 5, 9, 13, 17}	28	{1}	(1, 7, 20)			
	{1, 3, 5, 9, 15, 17}	28	{1}	(1, 2, 25)	(1, 10, 17)	(2, 7, 19)	
	{1, 3, 5, 13, 17, 19}	28	{1}				
	{1, 3, 5, 15, 17, 19}	7	{1, 15}	(1, 12, 15)			
	{1, 5, 9, 13, 17, 25}	4	Φ				
	{1, 9, 11, 15, 23, 25}	7	Φ				
36	{1, 5, 7, 11, 13, 17}	36	{1, 17}	(1, 1, 34)	(1, 17, 18)		
	{1, 5, 7, 11, 13, 19}	36	{1}	(1, 4, 31)	(1, 8, 27)		
	{1, 5, 7, 11, 19, 23}	36	{1}	(1, 2, 33)	(1, 8, 27)	(2, 11, 23)	
	{1, 5, 7, 13, 17, 25}	36	{1}	(1, 3, 32)	(1, 9, 26)	(3, 16, 17)	
	{1, 5, 7, 13, 19, 25}	36	{1}	(1, 6, 29)	(2, 3, 31)		
	{1, 5, 7, 19, 23, 25}	9	{1, 19}	(1, 16, 19)			
	{1, 5, 13, 17, 25, 29}	4	Φ				
	{1, 7, 13, 19, 25, 31}	3	Φ				

References

[1] Aoki, N., On some arithmetic problems related to the Hodge cycles on the Fermat varieties, Math. Ann., **266** (1983), 23–54. (Erratum: Math. Ann. 267 (1984), p. 572.)

[2] Aoki, N., Some new algebraic cycles on Fermat varieties, J. Math. Soc. Japan, **39** (1987), 385–396.

[3] Aoki, N., Simple factors of the jacobian of a Fermat curve and the Picard number of a product of Fermat curves, Amer. J. Math., **113** (1991), 779–833.

[4] Hazama, F., Algebraic cycles on certain abelian varieties and powers of special surfaces, J. Fac. Sci. Univ. Tokyo, **31** (1985), 487–520.

[5] Ran, Z., Cycles on Fermat hypersurfaces, Compositio Math., **42** (1981), 121–142.

[6] Ribet, K. A., Division fields of abelian varieties with complex multiplication, Soc. Math. France Mémorie, **2** (1980), 75–94.

[7] Shimura, G. and Taniyama, Y., *Complex multiplication of abelian varieties and its applications to number theory*, Math. Soc. Japan, 1961.

[8] Shioda, T., The Hodge conjecture for Fermat varieties, Math. Ann., **245** (1979), 175–184.

[9] Shioda, T., Algebraic cycles on abelian varieties of Fermat type, Math. Ann., **258** (1981), 65–80.

[10] Shioda, T. and Katsura, T., On Fermat varieties, Tôhoku Math. J., **31** (1979), 97–115.

[11] Yamamoto, K., The gap group of multiplicative relationship of Gauss sums, Symp. Math., **XV** (1975), 427–440.

Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Tokyo, 117–8501 Japan
e-mail address: aoki@rkmath.rikkyo.ac.jp